Дата-центр. Режим доступа:https://wiki2.org/ru/Дата-центр.

Основные факторы, влияющие на обеспечение информационной безопасности таможенных органов. Основные угрозы информационной безопасности таможенных органов

Данилова М.С.
Научный руководитель: Ковалькова И.А
Белорусский национальный технический университет

Защита информации – это деятельность по предотвращению утечки защищаемой информации, несанкционированного и непреднамеренного воздействий на защищаемую информацию.

Информационная безопасность – защищённость информации от незаконного ознакомления, преобразования, уничтожения, а также защищённость информации от воздействий, направленных на нарушение их работоспособности.

Безопасная информационная система – это система, которая:

защищает данные от несанкционированного доступа;

всегда готова предоставить данные своим пользователям;

надёжно хранит информацию и гарантирует неизменность данных.

Сущность обеспечения информационной безопасности таможенных органов отражена в «Основных направлениях развития таможенной службы Республики Беларусь», утверждённых приказом председателя Государственного Таможенного комитета от 08.04.2011 № 125-ОД.

Обеспечение информационной безопасности – проведение единой политики в области охраны и защиты информационных ресурсов и информации, система мер организационного, технического и иного характера, адекватных угрозам информационным ресурсам таможенных органов, техническим и программным средствам информационных технологий и, как следствие, интересам таможенных органов в целом[3].

Однако возникают факторы, которые необходимо учитывать при анализе реального состояния информационной безопасности и выявления ключевых проблем в этой области.

К таким факторам можно отнести:

ослабление контроля со стороны руководителей таможенных органов и их структурных подразделений за состоянием информационной безопасности, выполнением подчинёнными должностными лицами регламентов, должностных инструкций, нормативно-правовых актов;

недостаточность развития системы подготовки и переподготовки кадров для таможенных органов в сфере обеспечения информационной безопасности;

недостаточное оснащение таможенных органов сертифицированными средствами защиты информации, что снижает эффективность использования применяемых при отдельных таможенных информационных технологиях средств и методов защиты информации;

отставание отечественных информационных технологий, которое вынуждает идти по пути закупок незащищённой импортной техники, из-за чего повышается вероятность несанкционированного доступа к обрабатываемой информации и возрастает зависимость таможенных органов Республики Беларусь от иностранных производителей компьютерной и телекоммуникационной техники, а также программного обеспечения[1].

Угроза – потенциальная возможность нарушения информационной безопасности, то есть конфиденциальности, доступности и целостности информации, а также возможность нелегального использования ресурсов сети.

Основными угрозами безопасности информационных и телекоммуникационных средств и систем таможенных органов могут являться:

нарушения технологии обработки информации ограниченного доступа, обрабатываемой в таможенных органах;

нарушение законных ограничений на распространение информации ограниченного доступа, обрабатываемой в таможенных органах;

противоправные сбор и использование информации ограниченного доступа, обрабатываемой в таможенных органах;

перехват информации в сетях передачи данных и на линиях связи, дешифрование этой информации или её подмена;

несанкционированный доступ к информации, находящейся в базах данных таможенных органов;

внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия;

разработка и распространение программ (компьютерных вирусов), нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации;

уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации связи;

внедрение электронных устройств для перехвата информации в технические средства обработки, хранения и передачи информации по каналам связи, а также в служебные помещения таможенных органов;

уничтожение, повреждение, разрушение или хищение машинных и других носителей информации;

использование несертифицированных отечественных и зарубежных информационных технологий, средств защиты информации, средств информатизации, телекоммуникации и связи при создании и развитии автоматизированных систем таможенных органов[2].

Анализ угроз информационной безопасности таможенных органов Республики Беларусь позволяет понять значение угроз в построении системы обеспечения информационной безопасности таможенных органов.

Реагирование на риски и вызовы в информационной сфере осуществляется всеми без исключения государственными органами и организациями в соответствии с областью их деятельности согласно непосредственному предназначению максимально полно и оперативно. Государство в лице этих государственных органов и организаций обеспечивает своевременное принятие мер безопасности, незамедлительно оповещает заинтересованные субъекты, минимизирует ущерб и локализует последствия, определяет причастных лиц и организации, накапливает опыт противодействия угрозам.

Литература

Г. М. Бровка, И. А. Ковалькова, А. Н. Шавель. Информационная безопасность в таможенных органах:Учебное пособие. – Минск, 2019. – С. 108-110.

Т. П. Лепа. Информационные технологии в таможенной сфере: Учебное пособие. – Иркутск, Издательство БГУ, 2016. – С. 85-86.

Основные направления развития таможенной службы Республики Беларусь // Утверждено Приказом председателя ГТК от 08.04.2011 № 125-ОД.

Программные закладки и методы защиты от них

Жадинец Я.А.

Научный руководитель: Ковалькова И.А.

Белорусский национальный технический университет

На сегодняшний день многие традиционные ресурсы нашего человечества постепенно утрачивают своё первоначальное значение. На новом этапе развития общества появляется новый ресурс –